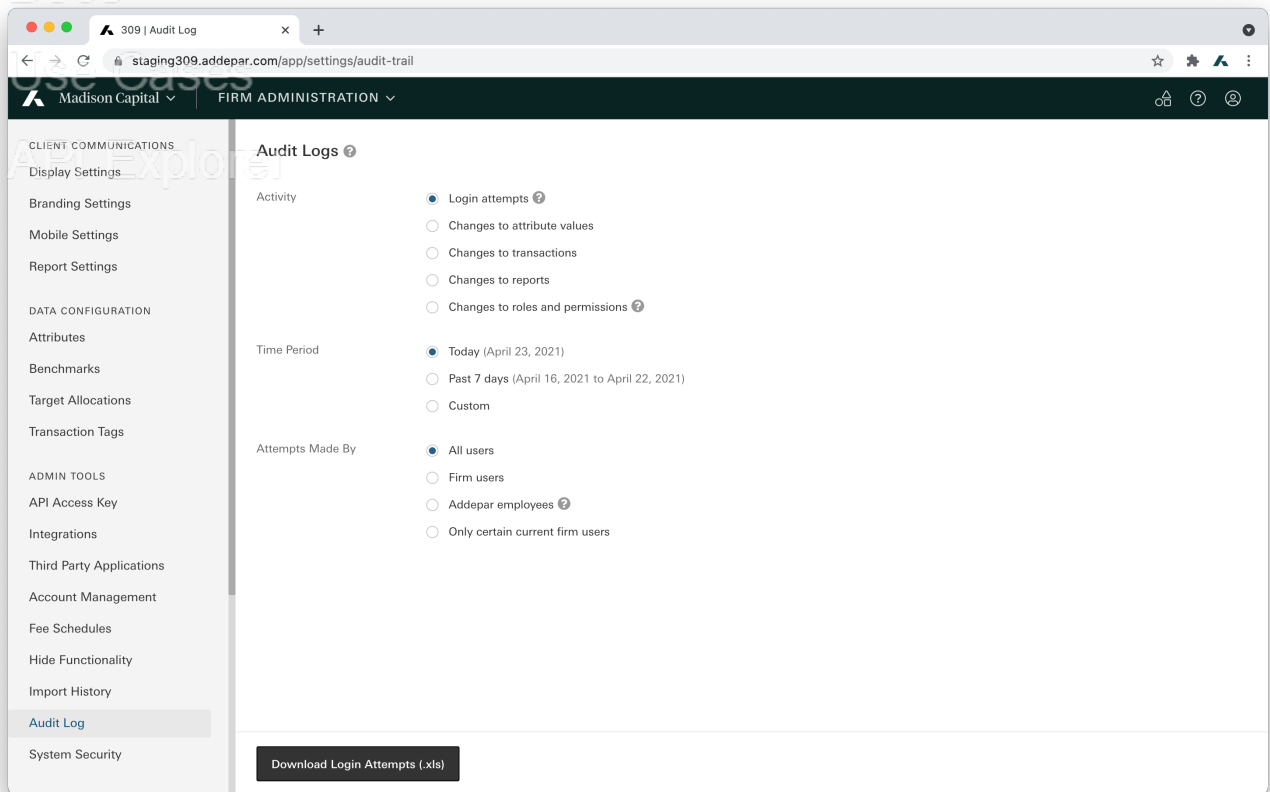




Audit

Audit logs track changes to attribute values, transactions, reports, and user roles and permissions. Each entry in a log represents an addition, modification, or deletion.



Audit logs can be downloaded directly in the application, or you can use the Audit API to retrieve the information.

Base Route	/v1/audit_trail
Endpoints	GET /v1/audit_trail/:id
Produces	POST /v1/audit_trail
Pagination	JSON
Produces	Yes
Application Permissions Required	"API Access: Create, edit, and delete" and "Manage firm settings: Audit logs"
OAuth Scopes	AUDIT_TRAIL

See login attempts

POST /v1/audit_trail

Retrieves a list of attempts by each user to sign into the application, Help Center, or Client Portal using Addepar credentials, SSO, or two-factor authentication.

Example

REQUEST

RESPONSE

POST https://examplefirm.addepar.com/api/v1/audit_trail

```
{
  "data": {
    "type": "audit_trail",
    "attributes": {
      "object_type": "login_attempt",
      "start_date": "2021-03-26",
      "end_date": "2021-03-30"
    }
  }
}
```

Request objects

REQUEST OBJECT	DESCRIPTION
	Required. Type of audit log you're retrieving.
object_type	Valid input: login_attempt
	Required. First date of the time period you want to audit.
	Valid formats: YYYY-MM-DD Example: 2021-01-01. Timezone is assumed to be UTC. YYYY-MM-DDThh:mm:ss followed by a timezone. Example 1: 2021-01-01T00:00:00Z timezone is UTC as specified by "Z". Example 2: 2021-01-01T00:00:00-05:00 timezone is EST as specified by offset -05:00.
start_date	
	If both start_date and end_date are missing, the time period will be today only. If one of them is missing, it will be set to equal the other one.
	You must specify both start_date and end_date if you want to use the YYYY-MM-DDThh:mm:ss format.
	Required. Last date of the time period you want to audit.
	Valid formats: YYYY-MM-DD Example: 2021-01-01. Timezone is assumed to be UTC. YYYY-MM-DDThh:mm:ss followed by a timezone. Example 1: 2021-01-01T00:00:00Z timezone is UTC as specified by "Z". Example 2: 2021-01-01T00:00:00-05:00 timezone is EST as specified by offset -05:00.
end_date	
	If both start_date and end_date are missing, the time period will be today only. If one of them is missing, it will be set to equal the other one.
	You must specify both start_date and end_date if you want to use the YYYY-MM-DDThh:mm:ss format.
	Operation performed.
actions	Valid input: Add
	If missing or empty, all actions will be included.
	Valid inputs: firmusers includes users at your firms addeparusers includes Addepar employees anyone includes all firm users and Addepar employees custom allows you to specify certain users
user_type	
users	List of IDs for the specific users you want to query. If user_type: custom but no users are specified, then all firm users will be included.

Response objects

RESPONSE OBJECT	DESCRIPTION
action	Operation performed.
performed_by_user_id	User ID of the person who attempted to sign in.
source	Manual indicates that the action was performed manually in the application. Import indicates the action was performed using the Import Tool.
	Indicates whether the attempt was successful.
	Outputs for attempts using Addepar credentials:
	locked_out
	password_incorrect
	successful
	username_invalid
status	Outputs for attempts using SSO:
	sso_successful
	sso_token_incorrect
	Outputs for attempts using two-factor authentication:
	two_factor_code_incorrect two_factor_successful two_factor_username_invalid
timestamp	Date and time the attempt was made (ISO 8601 format) based on your firm's timezone.

Response codes:

- 200 OK: Success
- 403 Forbidden: User does not have permission to see audit trails

See changes to attribute values

POST /v1/audit_trail

Retrieves a list user changes to attribute values applied at the asset- and position-level. You have the option to specify which actions you want to query.

Example

REQUEST	RESPONSE
POST https://examplefirm.addepar.com/api/v1/audit_trail	 <pre>{ "data": { "type": "audit_trail", "attributes": { "object_type": "attribute", "start_date": "2021-02-01", "end_date": "2021-02-02", "actions": ["Add"] } } }</pre>

Request objects

REQUEST OBJECT	DESCRIPTION
	Required. Type of audit log you're retrieving.
object_type	Valid input: attribute
	Required. First date of the time period you want to audit.
	Valid formats: YYYY-MM-DD Example: 2021-01-01. Timezone is assumed to be UTC. YYYY-MM-DDThh:mm:ss followed by a timezone. Example 1: 2021-01-01T00:00:00Z timezone is UTC as specified by "Z". Example 2: 2021-01-01T00:00:00-05:00 timezone is EST as specified by offset -05:00.
start_date	
	If both start_date and end_date are missing, the time period will be today only. If one of them is missing, it will be set to equal the other one.
	You must specify both start_date and end_date if you want to use the YYYY-MM-DDThh:mm:ss format.
	Required. Last date of the time period you want to audit.
	Valid formats: YYYY-MM-DD Example: 2021-01-01. Timezone is assumed to be UTC. YYYY-MM-DDThh:mm:ss followed by a timezone. Example 1: 2021-01-01T00:00:00Z timezone is UTC as specified by "Z". Example 2: 2021-01-01T00:00:00-05:00 timezone is EST as specified by offset -05:00.
end_date	
	If both start_date and end_date are missing, the time period will be today only. If one of them is missing, it will be set to equal the other one.
	You must specify both start_date and end_date if you want to use the YYYY-MM-DDThh:mm:ss format.
	Operation performed.
	Valid inputs: Add Modify Remove
actions	
	If missing or empty, all actions will be included.
	Valid inputs: firmusers includes users at your firms addeparusers includes Addepar employees anyone includes all firm users and Addepar employees custom allows you to specify certain users
user_type	
users	List of IDs for the specific users you want to query. If user_type: custom but no users are specified, then all firm users will be included.

Response objects

RESPONSE OBJECT	DESCRIPTION
	Operation performed.
action	<p>Outputs for changes to attributes applied at the entity-level:</p> <ul style="list-style-type: none"> add_entity_attribute modify_entity_attribute remove_entity_attribute <p>Outputs for changes to attributes applied at the position-level:</p> <ul style="list-style-type: none"> add_position_attribute modify_position_attribute remove_position_attribute
attribute_name	Name of the attribute.
entity_name	Name of the entity. Only applicable for changes to attributes at the entity-level.
entity_type	Type of entity. Only applicable for changes to attributes at the entity-level.
new_value	Value after the change was made. Empty for remove_entity_attribute and remove_position_attribute actions.
object_id	Attribute's unique identifier.
old_value	Value before the change was made. Empty for add_entity_attribute and add_position_attribute actions.
owned_id	Unique identifier of the asset where the attribute is applied. Only applicable for changes to attributes at the position-level.
owned_name	Name of the asset where the attribute is applied. Only applicable for changes to attributes at the position-level.
owned_type	Type of entity where the attribute is applied. Only applicable for changes to attributes at the position-level.
owner_id	Unique identifier of the entity that directly owns the asset where the attribute is applied. Only applicable for changes to attributes at the position-level.
owner_name	Name of the entity that directly owns the asset where the attribute is applied. Only applicable for changes to attributes at the position-level.
owner_type	Name of the entity that directly owns the asset where the attribute is applied. Only applicable for changes to attributes at the position-level.
performed_by_user_id	User ID of the person who made the change.
source	Manual indicates that the action was performed manually in the application. Import indicates the action was performed using the Import Tool.
timestamp	Date and time the change was made (ISO 8601 format) based on your firm's timezone.

Response codes:

- 200 OK: Success
- 403 Forbidden: User does not have permission to see audit trails

See changes to transactions, snapshots, and valuations

POST /v1/audit_trail

Retrieves a list user changes to transactions, snapshots, and valuations. You have the option to specify which actions you want to query.

Example

REQUEST	RESPONSE
---------	----------

POST https://examplefirm.addepar.com/api/v1/audit_trail



```
{
  "data": {
    "type": "audit_trail",
    "attributes": {
      "object_type": "transaction",
      "start_date": "2021-03-15",
      "end_date": "2021-04-30",
      "actions": ["Modify"]
    }
  }
}
```

Request objects

REQUEST OBJECT	DESCRIPTION
	Required. Type of audit log you're retrieving.
object_type	Valid input: transaction
	Required. First date of the time period you want to audit.
	Valid formats: YYYY-MM-DD Example: 2021-01-01. Timezone is assumed to be UTC. YYYY-MM-DDThh:mm:ss followed by a timezone. Example 1: 2021-01-01T00:00:00Z timezone is UTC as specified by "Z". Example 2: 2021-01-01T00:00:00-05:00 timezone is EST as specified by offset -05:00.
start_date	
	If both start_date and end_date are missing, the time period will be today only. If one of them is missing, it will be set to equal the other one.
	You must specify both start_date and end_date if you want to use the YYYY-MM-DDThh:mm:ss format.
	Required. Last date of the time period you want to audit.
	Valid formats: YYYY-MM-DD Example: 2021-01-01. Timezone is assumed to be UTC. YYYY-MM-DDThh:mm:ss followed by a timezone. Example 1: 2021-01-01T00:00:00Z timezone is UTC as specified by "Z". Example 2: 2021-01-01T00:00:00-05:00 timezone is EST as specified by offset -05:00.
end_date	
	If both start_date and end_date are missing, the time period will be today only. If one of them is missing, it will be set to equal the other one.
	You must specify both start_date and end_date if you want to use the YYYY-MM-DDThh:mm:ss format.
	Operation performed.
	Valid inputs: Add Modify Remove
actions	
	If missing or empty, all actions will be included.
	Valid inputs: firmusers includes users at your firms addeparusers includes Addepar employees anyone includes all firm users and Addepar employees custom allows you to specify certain users
user_type	
users	List of IDs for the specific users you want to query. If user_type: custom but no users are specified, then all firm users will be included.

Response objects

RESPONSE OBJECT	DESCRIPTION
	Operation performed.
	Outputs for changes to transactions: add_transaction modify_transaction remove_transaction
action	Outputs for changes to snapshots: add_snapshot modify_snapshot remove_snapshot
	Outputs for changes to valuations: add_valuation modify_valuation remove_valuation
new_value	Value after the change was made. Empty for the following actions: remove_transaction remove_snapshot remove_valuation
old_value	Value before the change was made. Empty for the following actions: add_transaction add_snapshot add_valuation
performed_by_user_id	User ID of the person who made the change.
source	Manual indicates that the action was performed manually in the application. Import indicates the action was performed using the Import Tool.
timestamp	Date and time the change was made (ISO 8601 format) based on your firm's timezone.
transaction_id	Unique identifier of the transaction. Only applicable for changes to transactions, not snapshots or valuations.

Response codes:

- 200 OK: Success
- 403 Forbidden: User does not have permission to see audit trails

See changes to reports

The Audit API is not currently available to retrieve changes to reports. You must use pull these audit logs directly from the application.

See changes to roles and permissions

POST /v1/audit_trail

Retrieves a list user changes to roles and user permissions.

Example

REQUEST	RESPONSE
---------	----------

POST https://examplefirm.addepar.com/api/v1/audit_trail



```
{
  "data": {
    "type": "audit_trail",
    "attributes": {
      "object_type": "permission",
      "start_date": "2021-03-15",
      "end_date": "2021-03-30"
    }
  }
}
```

Request objects

REQUEST OBJECT	DESCRIPTION
	Required. Type of audit log you're retrieving.
object_type	Valid input: permission
	Required. First date of the time period you want to audit.
	Valid formats: YYYY-MM-DD Example: 2021-01-01. Timezone is assumed to be UTC. YYYY-MM-DDThh:mm:ss followed by a timezone. Example 1: 2021-01-01T00:00:00Z timezone is UTC as specified by "Z". Example 2: 2021-01-01T00:00:00-05:00 timezone is EST as specified by offset -05:00.
start_date	
	If both start_date and end_date are missing, the time period will be today only. If one of them is missing, it will be set to equal the other one.
	You must specify both start_date and end_date if you want to use the YYYY-MM-DDThh:mm:ss format.
	Required. Last date of the time period you want to audit.
	Valid formats: YYYY-MM-DD Example: 2021-01-01. Timezone is assumed to be UTC. YYYY-MM-DDThh:mm:ss followed by a timezone. Example 1: 2021-01-01T00:00:00Z timezone is UTC as specified by "Z". Example 2: 2021-01-01T00:00:00-05:00 timezone is EST as specified by offset -05:00.
end_date	
	If both start_date and end_date are missing, the time period will be today only. If one of them is missing, it will be set to equal the other one.
	You must specify both start_date and end_date if you want to use the YYYY-MM-DDThh:mm:ss format.
	Operation performed.
	Valid inputs: Add Modify Remove
action	
	If missing or empty, all actions will be included.
	Valid inputs: firmusers includes users at your firms addeparusers includes Addepar employees anyone includes all firm users and Addepar employees custom allows you to specify certain users
user_type	
	List of IDs for the specific users you want to query. If user_type: custom but no users are specified, then all firm users will be included.
users	

Response objects

RESPONSE OBJECT	DESCRIPTION
action	Operation performed.
new_value	Value after the change was made.
old_value	Value before the change was made.
performed_by_user_id	User ID of the person who made the change.
source	<code>Manual</code> indicates that the action was performed manually in the application. <code>Import</code> indicates the action was performed using the Import Tool.
timestamp	Date and time the change was made (ISO 8601 format) based on your firm's timezone.
user_email	Email address of the user.
user_id	User ID of the user.
user_name	Name of the user.

Response codes:

- 200 OK: Success
- 403 Forbidden: User does not have permission to see audit trails

Get details about a specific Audit Log Entry ID

GET `/v1/audit_trail/:id`

Retrieves details about a specific user action. Use the endpoints listed above to get the entry ID.

Example

REQUEST	RESPONSE
GET https://examplefirm.addepar.com/api/v1/audit_trail/AXfSBFEeYH1_Q0j5iIH	

Response codes

- 200 OK: Success
- 403 Forbidden: User does not have permission to see the audit trail
- 404 Not Found: No audit trail found or non-permissioned audit trail ID



Addepar is a wealth management platform that specializes in data aggregation, analytics and performance reporting.

OUR APIS

Attributes API

Entities API

DEVELOPERS

Documentation

API Explorer

[Entity Types API](#)

[Files API](#)

[Groups API](#)

[Jobs API](#)

[Portfolio API](#)

[Positions API](#)

[Roles API](#)

[Transactions API](#)

[Users API](#)

MORE

[Addepar Home](#)

[Engineering Blog](#)

[Integrations](#)

[Contact Us](#)

[Partner with Addepar](#)

© 2021 Addepar, Inc. All rights reserved.

[Privacy Policy](#)

[Terms of Use](#)

